Introduction to the Security of Pathogens in Laboratory Environments

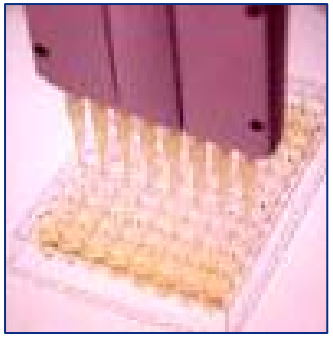
Jennifer Gaudioso, Ph.D.
Sandia National Laboratories

Seminar on Prevention and Crisis Management of Bioterrorism
Southeast Asia Regional Centre
for Counter-Terrorism, Malaysia
July 19, 2005

SAND No. 2005-4328C
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Challenges to Securing Biological Agents

- **Dual-use characteristics**
  - Valuable for many legitimate, defensive, and peaceful commercial, medical, and research applications
- **Nature of the material**
  - Living and self-replicating organisms
  - Used in very small quantities
  - Cannot be reliably quantified
  - Exist in many different process streams in facilities
  - Contained biological samples are virtually undetectable using standoff technologies
- **Laboratory "culture"**
  - Biological research communities not accustomed to operating in a security conscious environment



Sandia National Laboratories

Security System Considerations

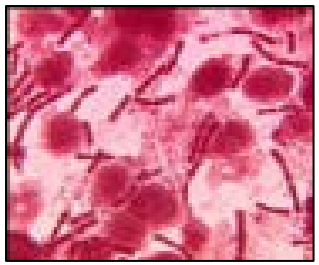
- **Cannot protect every asset against every conceivable threat**
- **Detection of theft extremely difficult**
  - **Microscopic**
  - **No detectable signature**
  - **Constantly changing quantities**
- **User input necessary**
  - **Minimize operational impacts**
  - **Integrate with biosafety systems**
- **Resources are limited and must be allocated effectively**
  - **Risk assessment and management**

Sandia National Laboratories

Risk Management

- Establishes which assets should be protected against which threats
  - Assets are items that are:
    - Dangerous
    - Hard to replace
    - Rare
    - Critical to operations
- Ensures that the amount of protection provided to a specific asset, and the cost for that protection, is proportional to the risk of the theft or destruction of that asset
- Begins with a risk assessment

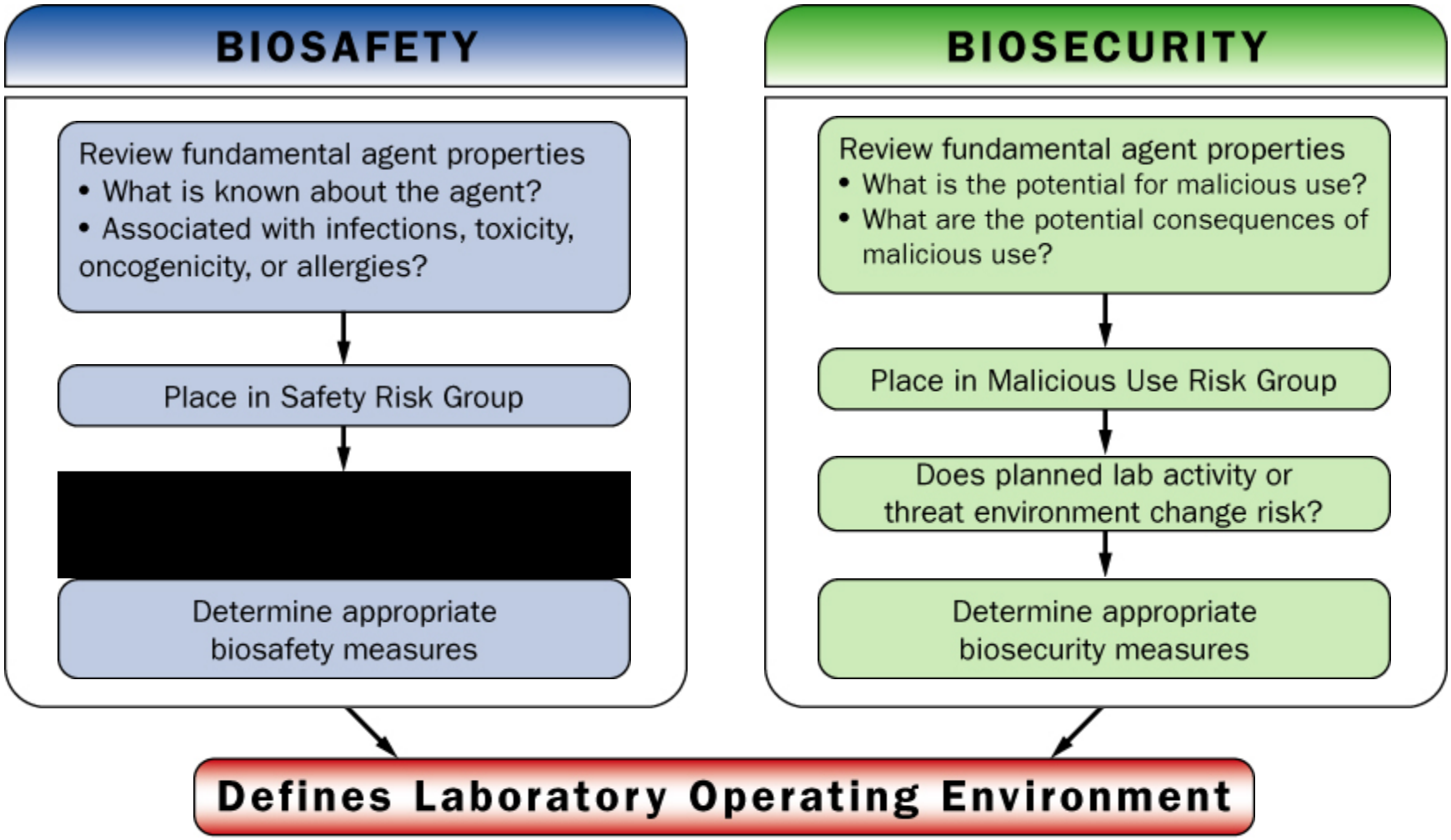
Biosecurity Risk Assessment



1. **Evaluate assets**
2. **Evaluate threat**
3. **Evaluate risk**

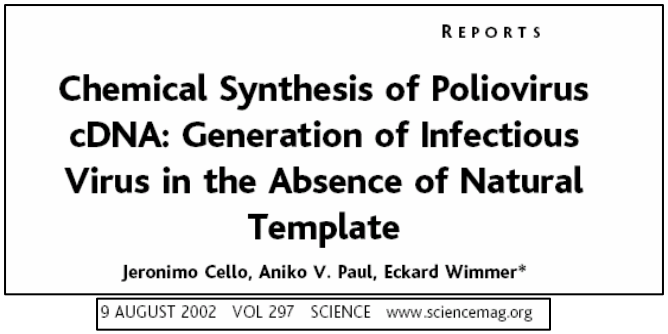
Sandia National Laboratories

Integrated Biosafety and Biosecurity



Malicious Use Risk Group Evaluation

- **Assess value of the agents from an adversary's perspective**
  - **Consequences**
    - Contagiousness
    - Medical effects (morbidity and mortality)
    - Potential to become endemic
    - Economic impact
  - **Weaponization potential**
    - Acquisition
    - Production
      - Ease of growth
      - Ease of processing
      - Ease of storage
    - Dissemination
      - Modes (e.g. Aerosol, Oral)
      - Environmental hardiness

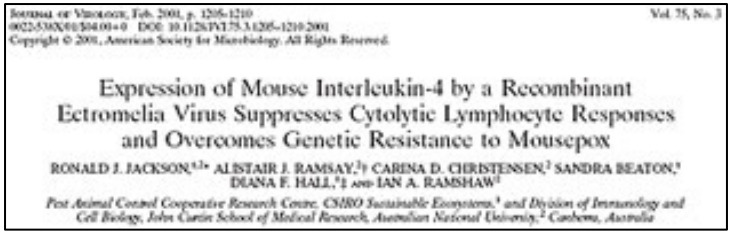


REPORTS

Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template

Jeronimo Cello, Aniko V. Paul, Eckard Wimmer*

9 AUGUST 2002 VOL 297 SCIENCE www.sciencemag.org



Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox

RONALD J. JACKSON, ALISTAIR J. RAMSAY, CARINA D. CHRISTENSEN, SANDRA BEATON, DIANA F. HALL, AND IAN A. RAMSHAW

Sandia National Laboratories

Malicious Use Risk Groups

- **Nonpathogenic**
  - **Malicious use would have insignificant or no consequences**
- **Low Malicious Use Risk (LMUR)**
  - **Difficult to deploy maliciously, and/or**
  - **Malicious use would have few consequences**

- **Moderate Malicious Use Risk (MMUR)**
  - **Relatively difficult to deploy maliciously, and**
  - **Malicious use would have localized consequences with low to moderate casualties and/or economic damage**
- **High Malicious Use Risk (HMUR)**
  - **Not particularly difficult to deploy maliciously, and**
  - **Malicious use could have national or international consequences, causing moderate to high casualties and/or economic damage**
- **Extreme Malicious Use Risk (EMUR)**
  - **Would normally be classified as HMUR, except that they are not found in nature (eradicated)**
  - **Could include genetically engineered agents, if they were suspected of being a HMUR**

Other Assets at Biological Facilities

- **Security Information or Systems**
  - **May be targeted to facilitate gaining access to dangerous biological materials**
- **Other Facility Assets**
  - **May be targeted by political extremists, disgruntled employees, etc.**
  - **May include:**
    - **High containment laboratories**
    - **Animals**

Elements That May Modify Risk

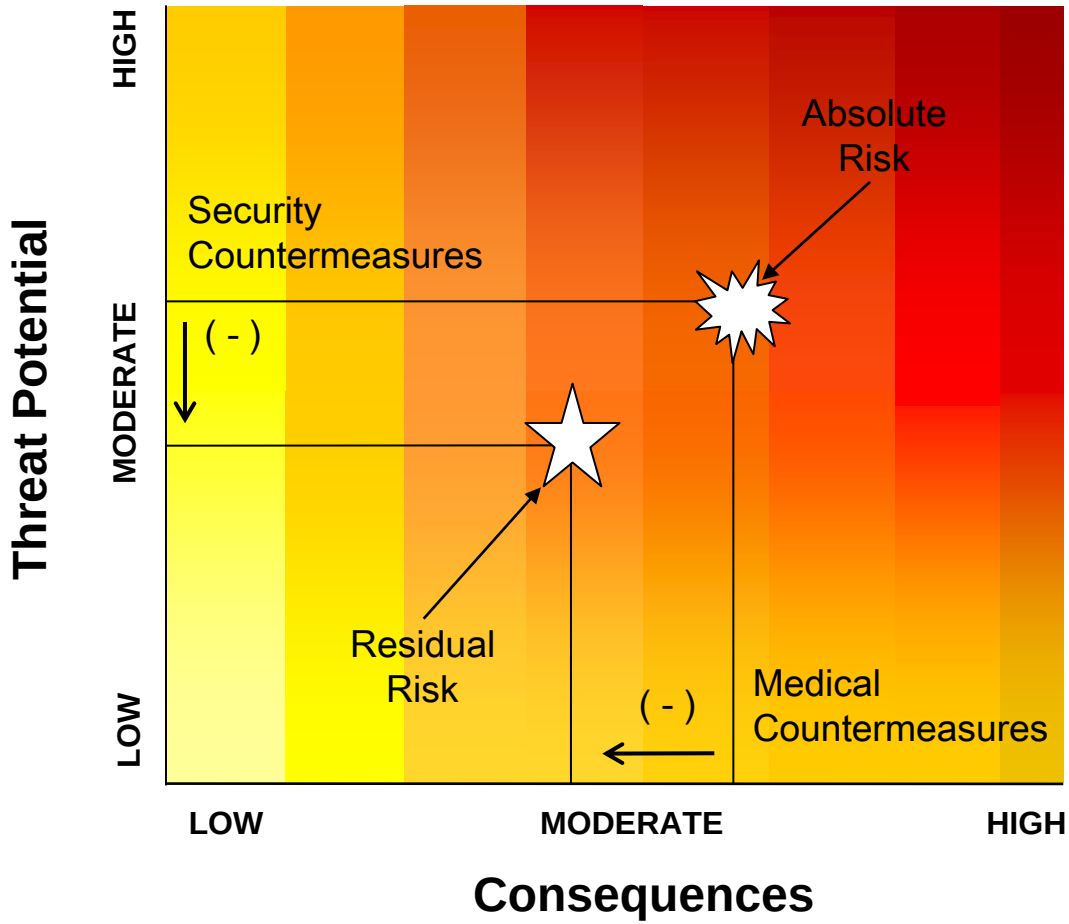
- **Consider lab experiment**
  - **Does planned experiment produce an agent with higher weaponization potential or higher potential consequences?**
- **Evaluate local threat environment**
  - **Insiders**
    - **Authorized access to the facility, dangerous pathogens, and/or restricted information**
  - **Outsiders**
    - **No authorized access**
  - **Evaluate threat potential of possible insiders and outsiders:**
    - **Motive**
    - **Means**
    - **Opportunity**

Sandia National Laboratories

Threat Potential

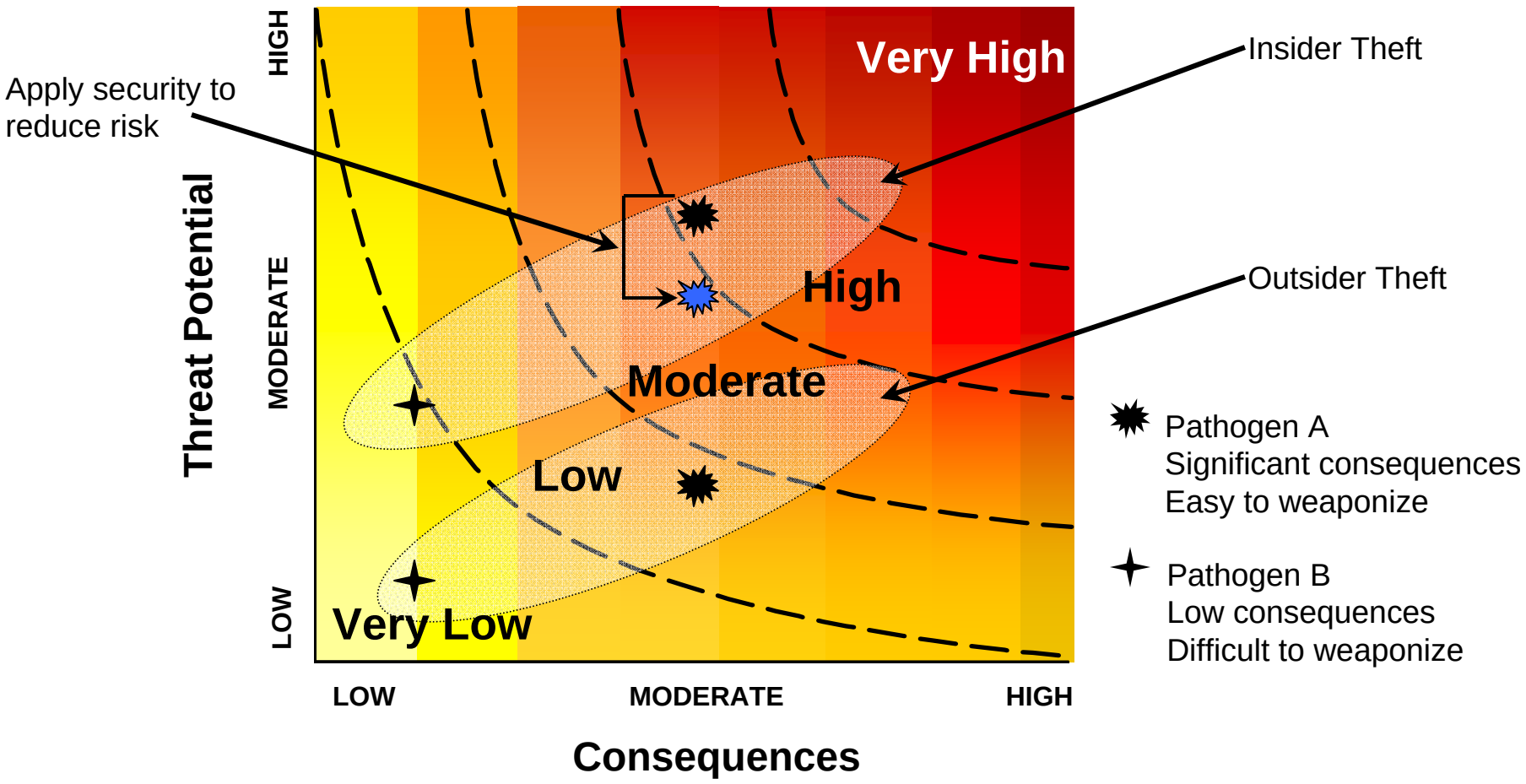
- **Motive**
  - **Asset Attractiveness**
    - **How well does the acquisition or sabotage of the asset achieve the adversary's objective, or lead to achieving the adversary's objective?**
- **Means**
  - **Capability**
    - **Does the adversary have the skills, knowledge, and tools necessary to conduct the attack/meet the objective?**
- **Opportunity**
  - **Environment**
    - **Is the adversary active in the area?**
    - **How recently have they acted in ways that may be threatening?**
    - **Has there been any indication of targeting?**

Biosecurity Risk Assessment and Mitigation



Sandia National Laboratories

Biosecurity Risk: Insider vs. Outsider Threat

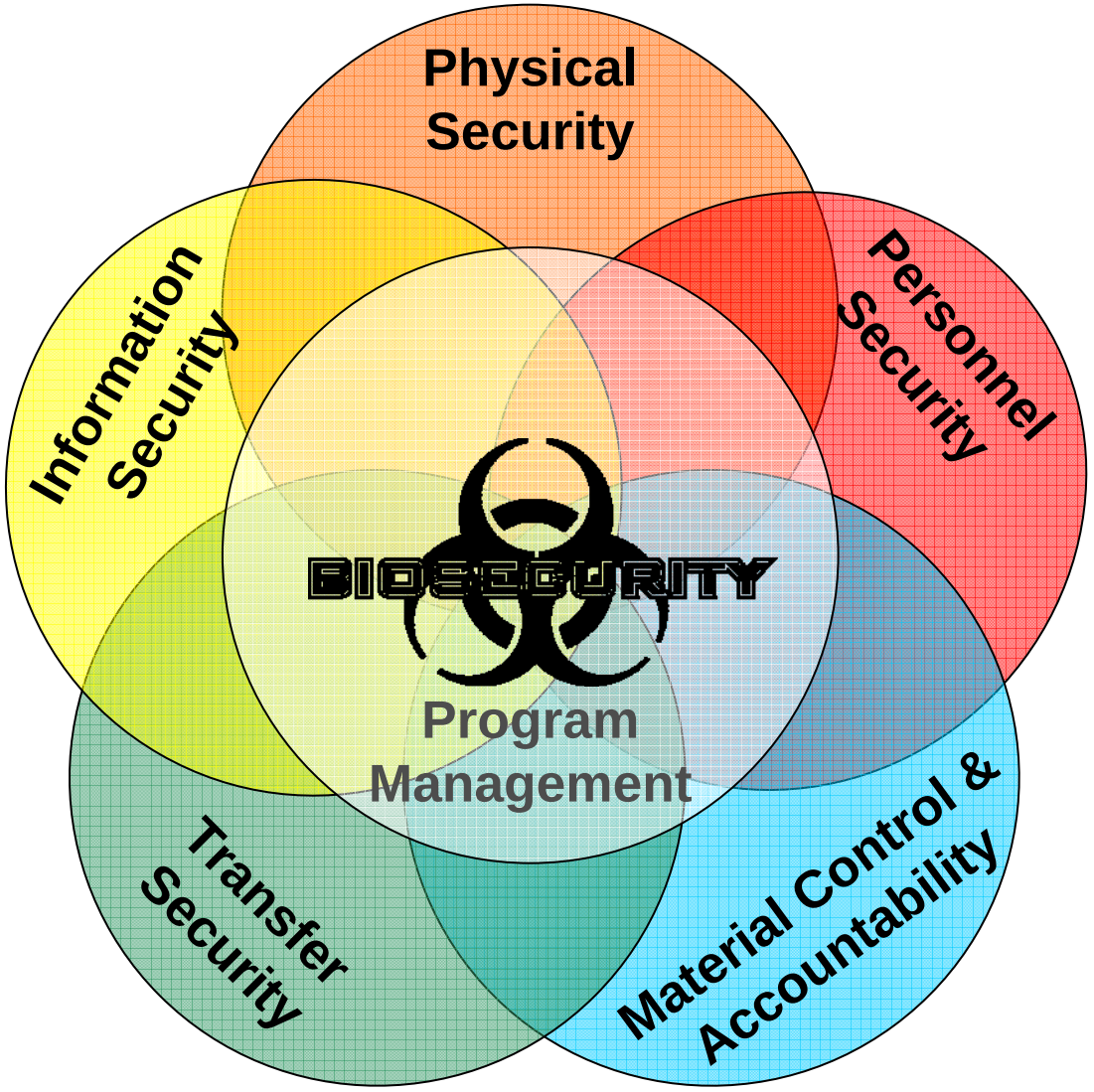


Sandia National Laboratories

Program Management: Responsibilities

- **Identify the protection objectives of the biosecurity system**
  - **Distinguish between “unacceptable” and “acceptable” risks**
  - **Ensure that the cost to protect an agent, is proportional to the risk of malicious use**
- **Design the system**
  - **Physical security**
  - **Security policies and procedures**
- **Write security and emergency response plans**
- **Conduct regular training and internal reviews**
- **Allocate resources**

Components of Biosecurity



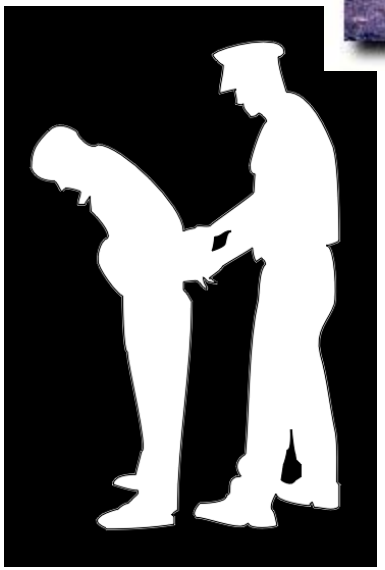
Sandia National Laboratories

Laboratory Biosecurity Plan

- **Develop laboratory biosecurity plan:**
  - **Facility mission and description**
  - **Risk definition(s)**
  - **Physical security**
  - **Personnel management**
  - **Material control and accountability**
  - **Material transfer security**
  - **Information security**
  - **Biosecurity program management**
  - **Incident response plans and reporting**

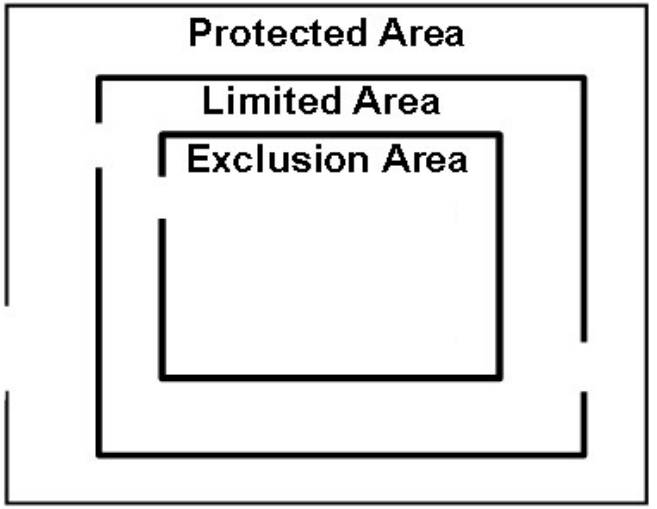
Elements of a Physical Security System

- Graded protection
- Access control
- Intrusion detection
- Response force



Graded Protection: Concentric Layers of Security

- **Property Protection Areas**
  - Low risk assets
    - Grounds
    - Public access offices
    - Warehouses
- **Limited Areas**
  - Moderate risk assets
    - Laboratories
    - Sensitive or administration offices
    - Hallways surrounding Exclusion Areas
- **Exclusion Areas**
  - High risk assets
    - High containment laboratories
    - Computer network hubs



Sandia National Laboratories

Physical Security

- **Access control**
  - **Ensures only authorized individuals are allowed entry**
    - **Increasingly strict controls as you move toward assets of highest risk**
    - **Unique credential: Grants access to specific areas by specific personnel**
- **Intrusion detection**
  - **Detect unauthorized access**
    - **Guards**
    - **Electronic sensors**
  - **Assessment**
    - **Validation of violation before response**
    - **Can be direct (guards) or remote (video)**
- **Response Force**
  - **On-site**
  - **Local law enforcement**

Personnel Security

- **Personnel Screening**
- **Badges**
- **Visitor Control**

Screening

- **Conduct screening for authorized individuals**
  - **Increasing level of scrutiny for high risk positions**
  - **Degree of scrutiny commensurate with need for unescorted access to restricted areas and/or materials**
- **Mechanisms:**
  - **Verify employment application information**
  - **Psychological/personality testing**
  - **Background investigation**

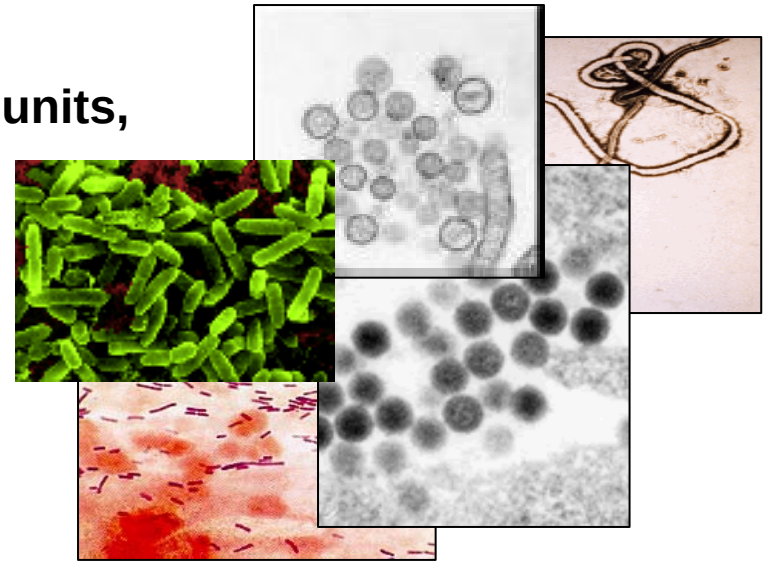
Badges and Visitor Controls

- **Badges**
  - **Should be issued to those individuals authorized to be on-site**
- **Visitors**
  - **Types**
    - **Personal Visitors, Casual Visitors, Working Visitors**
  - **Controls**
    - **All visitors should have a host at the facility**
    - **Visitors should be escorted in restricted areas**

Sandia National Laboratories

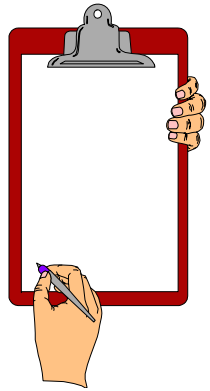
Material Control and Accountability

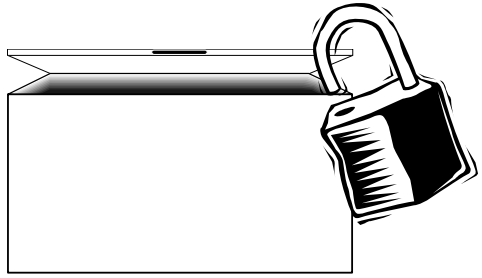
- Defining “material” is complicated
- Agent
  - Name and description
- Quantity
  - Based on containers or other units, NOT number of microbes



Material Control and Accountability

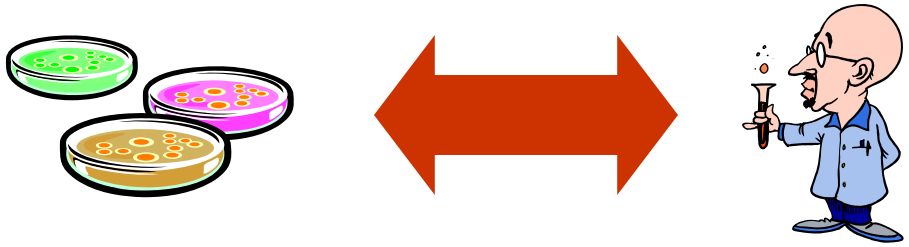
- Control is either…
  - Engineered / Physical
  - Administrative
- Containment is part of material control
  - Containment Lab / Freezer / Ampoule
- Procedures are essential for material control
  - For both normal and abnormal conditions





Material Control and Accountability

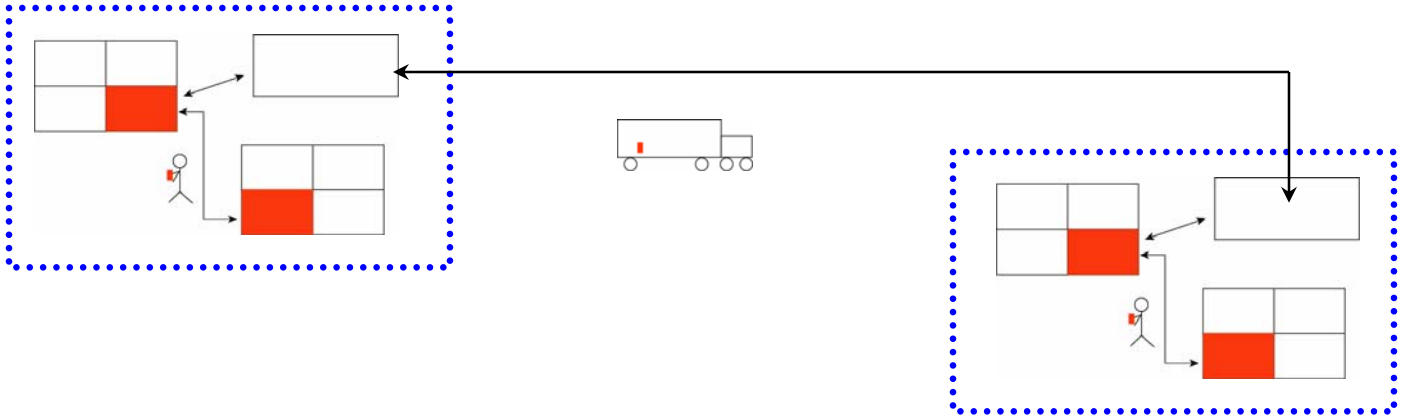
- **All material should have an associated “accountable person”**



- **Procedures should ensure accountability**

Material Transport Security

- **Why?**
  - **Dangerous pathogens and toxins are vulnerable to theft during movement outside of protected areas**
- **Who?**
  - **Facilities, carriers, and states all responsible**
- **The goal of transport security is**
  - **To mitigate the risk of theft during transport**



Chain of Custody

- Aims to protect sample by documenting
  - All individuals who have control of sample
  - Secure receipt of material at appropriate location
- Chain of custody documentation includes
  - Description of material being moved
  - Contact information for a responsible person
  - Time/date signatures of every person who assumes control

Transport Responsibilities at Facility

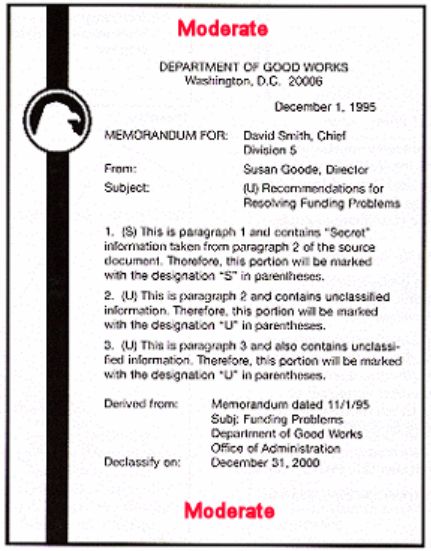
- **Personnel management**
  - **For people who have access to dangerous pathogens and toxins or information during transfers**
- **Establish chain of custody**
  - **Record all individuals who have contact with the dangerous pathogens and toxins**
- **Provide physical security**
  - **For packages that need temporary storage**
- **Protect transport documentation**
- **Determine who is able to authorize, transport, and receive dangerous pathogens and toxins**

Information Security

- Protect information that is too sensitive for public distribution
  - Label information as restricted
  - Limit distribution
  - Restrict methods of communication
  - Implement network and desktop security
- Types of sensitive information
  - Security of dangerous pathogens and toxins
    - Risk assessments
    - Security system design
    - Access authorizations
  - Personnel records
  - Financial records

Identification, Control, and Marking

- **Identification**
  - **Users of information should know the information's designated sensitivity level**
  - **Levels of sensitivities should be based on standards**
  - **A review and approval process aids in the identification of sensitivities**
- **Control**
  - **The control of moderately and highly sensitive information should be the direct responsibility of the individual with the information**
  - **This includes the physical security of the information and places where the information is stored**
- **Marking**
  - **Moderately and highly sensitive information should be labeled in a consistent manner**
  - **Marking and control methods should be well understood by those working with information**



Moderate

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

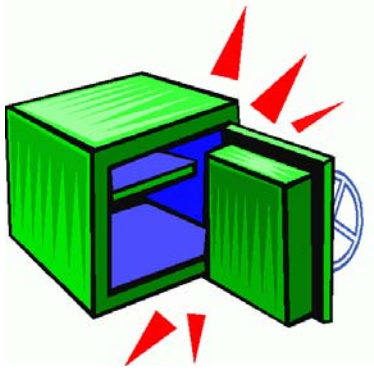
2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95
Subj: Funding Problems
Department of Good Works
Office of Administration

Declassify on: December 31, 2000

Moderate



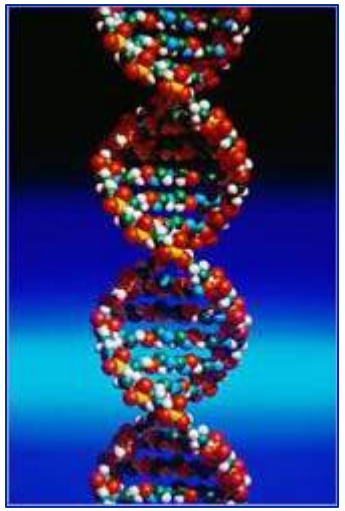
Sandia National Laboratories

Communication and Network Security

- **Insecure transmission of information can lead to accidental release**
  - **Mail, email, or fax security is required**
  - **Limited discussions in open areas**
  - **Information should only be reproduced when needed and each copy must be controlled as the original**
- **Network Management**
  - **The network on which all information is transmitted and systems on the network should be protected**
    - **Infrastructure**
    - **Servers**
    - **Network layered access**
    - **Desktop security**
    - **Remote access**
    - **Wireless**

Summary

- **Necessary to take steps to reduce the likelihood that the *high risk agents* could be stolen from bioscience facilities**
- **Critical that these steps are designed specifically for biological materials and research so that the resulting system will balance science and security concerns**
- **WHO and other international organizations developing guidance on Laboratory Biosecurity that provides an overview of these principles**



Contact Information

Jennifer Gaudioso, Ph.D.
Sandia National Laboratories
PO Box 5800, MS 1371
Albuquerque, NM 87185
USA
Tel. 505-284-9489
email: jmgaudi@sandia.gov

www.biosecurity.sandia.gov

Sandia National Laboratories